How can I manage validation and decryption of S/MIME encoded emails?

Julien Ducro - 2018-03-14 - Comments (0) - Using Deskpro

Context

With the usage of an email certificate, you can ensure that your email communication is not tampered with and even encrypt the content so confidential data cannot be intercepted.

Getting a certificate

Several providers can deliver you an email certificate corresponding to your email address, you can get one for free on Comodo.

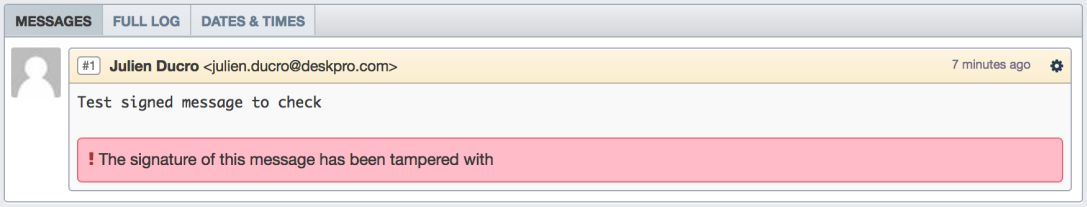
Email Signature

If you configure your email client you can sign your emails, which means adding an attachment that encrypts the original content of the email.

When the email is delivered the recipient compares the content with the signature and checks everything was delivered as it should be.

In Deskpro we add the following message to distinguish if the checks have passed:

In the below case we add this error message to show the signature didn't match the content:



This means that the content has been altered or that the signature is corrupted. Common causes can be data corruption, user error and time not being properly set.

Email encryption

To encrypt emails you need to add the public certificate of your recipient in your system.

The content will then be unreadable to anyone who doesn't have the private key needed to decrypt it.

Set up

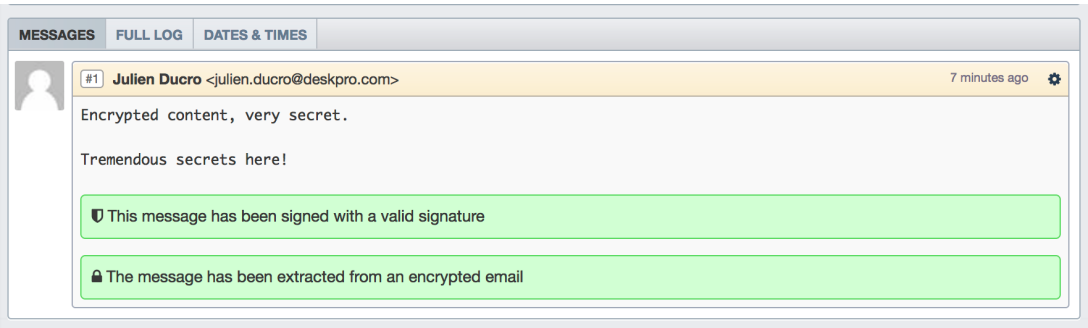
Go to **Admin > Tickets > Email Accounts** and select the target email account.

Under *Account Details* select *Advanced Options*

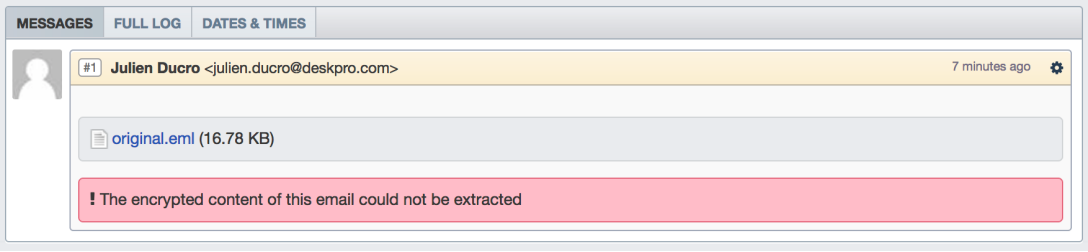
Upload your certificate and key.

Decrypted emails

If you send an encrypted email to Deskpro and its content is sucessfully decrypted with the key stored on the server, it will be shown like a regular message with an additional message to inform you (this email was also signed):



In the case of a failure of the decryption you will be provided with the below message. You can then try to open this in your email client.



Tags

email

encryption

signature